von Rechtsanwalt **Phil Salewski**

# Online-Shop gehackt -was nun?: Anleitung für eine DSGVO-konforme Reaktion auf Datenpannen im Online-Shop mit Musterbenachrichtigung

Schon nach der bisherigen Rechtslage waren Online-Händler wie alle anderen Verantwortlichen auch dazu verpflichtet, durch geeignete technische und organisatorische Maßnahmen die Sicherheit und Vertraulichkeit der von ihnen verarbeiteten Daten zu gewährleisten und so ihre Systeme gegen ein Durchsickern oder freies Verfügbarwerden von personenbezogenen Informationen zu wappnen. Dies wird sich auch unter der ab dem 25.05.2018 geltenden DSGVO nicht ändern. Allerdings sieht der neue Rechtsakt für Fälle derartiger Datenpannen eine Benachrichtigungspflicht gegenüber der Meldebehörde und gegebenenfalls des Betroffenen vor. Aufgrund der hierbei einzuhaltenden kurzen Frist sollte der Händler vorbereitet sein. Nachstehend zeigt die IT-Recht Kanzlei auf, wie auf Datenpannen angemessen zu reagieren ist und stellt ihren Mandanten ein Muster für die obligatorische Benachrichtigung bereit.

## I. Datenpannen im Online-Shop

Datenpannen sind Verletzungen des Schutzes personenbezogener Daten, die durch ein Versagen oder eine unzureichende Implementierung von angemessenen technischen und organisatorischen Maßnahmen entstehen. Im Internet bestehen derartige Verletzungen insbesondere darin, dass Daten von einem Verantwortlichen so gespeichert und verfügbar gehalten werden, dass Dritte ungehindert auf diese zugreifen können. Auch denkbar sind aber gezielte Hacking-Angriffe auf Shop-Systeme. Die Auswirkungen sind regelmäßig katastrophal, weil sensible private Informationen einem weltweiten Publikum zugänglich gemacht werden und so Missbrauch und Piraterie alle Tore und Türen geöffnet werden.

Datenlecks in Online-Shops können aufgrund der Art und Anzahl der zu Kunden gespeicherten Informationen in Form von gebündelten Adress-, Mail- und Zahlungsdaten zu besonders gravierenden Beeinträchtigungen für die betroffenen Kunden führen und diese erheblichen Risiken finanzieller und persönlichkeitsrechtlicher Ausbeutung aussetzen.

Aus diesem Grund sind Online-Händler nach Art. 32 DSGVO grundsätzlich gehalten, Datenpannen durch geeignete Maßnahmen präventiv entgegenzuwirken, und gespeicherte Datensätze insbesondere zu verschlüsseln sowie deren Speicherorte und Verarbeitungssysteme mit Zugriffspasswörtern und Firewalls zu schützen.

## II. Leck entdeckt – was nun?

Sollte sich trotz oder mangels hinreichender technischer und organisatorischer Maßnahmen im Shop eine Datenpanne durch Leck oder Hacking ergeben, durch die Kundendaten unbefugten Dritten oder der Allgemeinheit zugänglich werden, ist der Händler ab Kenntnis der Datenverletzung nach Art. 33 ff. DSGVO zu verschiedenen unmittelbaren Reaktionen verpflichtet. Unterbleiben diese Reaktionen, kann der Händler gemäß Art. 83 Abs. 4 lit. a DSGVO mit empfindlichen bis existenzbedrohenden Geldbußen belegt werden.

### 1.) Behebung der Panne

Zunächst muss der Händler unverzüglich und im Rahmen des ihm Möglichen versuchen, die Datenpanne so zu beheben, dass von Ihr keine Gefahren mehr für den Schutz der betroffenen personenbezogenen Daten ausgehen. Maßnahmen sind hier insbesondere die sofortige nachträgliche Verschlüsselung, die Einrichtung bzw. Wiederherstellung von Zugriffssperren und – falls die Beeinträchtigung nicht auf andere Weise abgestellt werden kann – ultimativ die Löschung der betroffenen Datensätze

### 2.) Benachrichtigung der Aufsichtsbehörde

Art. 33 DSGVO verpflichtet Verantwortliche dazu, innerhalb von 72 Stunden **nach Kenntniserlangung** von der Datenpanne die für sie zuständige Aufsichtsbehörde über die Verletzung zu benachrichtigen, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Sofern die Datenpanne im Online-Shop die Kundendaten von Privatpersonen betrifft, ist ein solches Risiko immer gegeben mit der Folge, dass die Meldepflicht eingreift.

Der zuständigen Aufsichtsbehörde gegenüber sind in der kurzen 3-Tagesfrist folgende Angaben zu machen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (sollte ein Datenschutzbeauftragter nicht bestellt werden müssen, sind Name und Kontaktdaten des Händlers anzugeben)
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der vom Händler ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Hinweis: die zuständige Aufsichtsbehörde ist die Datenschutzbehörde des Bundeslandes, in welchem der Online-Händler seinen Sitz hat.

Kann der Online-Händler der Meldepflicht nicht innerhalb von 3 Tagen nach Kenntniserlangung Folge leisten, so muss der verspäteten Meldung eine Begründung für die Verzögerung beigefügt werden.

Kann der Online-Händler der Benachrichtigung aus tatsächlichen Gründen nicht sofort alle erforderlichen Bestandteile beifügen, so wahrt er die 3-Tagesfrist gemäß Art. 33 Abs. 4 DSGVO auch dann, wenn lediglich das Auftreten der Datenpanne gemeldet wird und die weiteren Pflichtinformationen ohne unangemessene weitere Verzögerung schrittweise nachgereicht werden.

Vor allem in Anbetracht der kurzen Meldefrist ist das Bereithalten einer Mustermeldung unbedingt empfehlenswert, in welche im Falle einer Datenpanne sodann allein die erforderlichen Eckdaten eingetragen werden müssen. Ein solches Muster kann unter III. abgerufen werden.

## 3.) Dokumentation der Datenpanne

Gemäß Art. 33 Abs. 5 DSGVO hat der Online-Händler die Datenpanne einschließlich aller im Zusammenhang mit ihr stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zwingend zu dokumentieren. Diese Dokumentation muss so detailliert sein, dass sie der Aufsichtsbehörde die Überprüfung der Einhaltung der Punkte 1) und 2) ermöglicht.

## 4.) Gegebenenfalls Benachrichtigung des Betroffenen

Dann, wenn die Datenpanne ein hohes Risiko in sich birgt, dass Rechte und Freiheiten von privaten Kunden beeinträchtigt werden, sind gemäß Art. 34 DSGVO zusätzlich zur Aufsichtsbehörde auch alle konkret Betroffenen in einfacher und verständlicher Art und Weise zumindest über Folgendes zu informieren:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (sollte ein Datenschutzbeauftragter nicht bestellt werden müssen, sind Name und Kontaktdaten des Händlers anzugeben)
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Hinweis: das Muster unter III. ist so formuliert, dass es auch dem jeweiligen Betroffenen weitergeleitet werden kann

Ein die zusätzliche Meldepflicht auslösendes hohes Risiko ist im Online-Shop vor allem dann anzunehmen, wenn Zahlungsdaten der Kunden oder als besonders sensibel geltende Gesundheitsdaten durchsickern und dem ungehinderten Zugriff Dritter zugänglich werden.

Die konkret Betroffenen sind unverzüglich, also ohne schuldhaftes Zögern, nach Kenntniserlangung von der Datenpanne zu informieren.

Zu beachten ist allerdings, dass gemäß Art. 33 Abs. 3 DSGVO die zusätzliche Benachrichtigungspflicht gegenüber Betroffenen entfällt, wenn

- der Online-Händler geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten nachträglich angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung oder
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht

Insbesondere in Fällen also, in denen der Händler nach Kenntniserlangung von der Datenpanne unverzüglich deren Abrufbarkeit gegenüber Unbefugten verhindert und demgemäß den Zugriff sperrt, sind die individuell Betroffenen nicht zu informieren.

Hinweis: die nachträgliche Abhilfe entbindet nur von der Meldepflicht gegenüber Betroffenen, nicht aber von derjenigen gegenüber der Behörde. Diese ist stets anzurufen.

## III. Musterbenachrichtigung der Aufsichtsbehörde bei festgestellter Datenpanne

Die IT-Recht Kanzlei stellt ihren Mandanten Muster zur Verfügung, die im Falle möglicher Datenpannen gegenüber den Kunden eingesetzt werden können. Selbstverständlich entsprechen diese Muster den Vorgaben der neuen Datenschutz-Grundverordnung.

Die Muster sind hier abrufbar.

Autor:
**RA Phil Salewski**
Rechtsanwalt